IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

Midwest American Federal Credit Union, *on behalf of itself and others similarly situated,* Plaintiff, v. Arby's Restaurant Group, Inc., Defendant.	Civil Action No. 1:17-CV-514-AT

FINANCIAL INSTITUTION PLAINTIFFS' CONSOLIDATED CLASS ACTION COMPLAINT

Plaintiffs are financial institutions (identified below) filing this Consolidated Class Action Complaint individually and on behalf of similarly situated banks, credit unions, and other payment card-issuing financial institutions against Defendant, Arby's Restaurant Group ("ARG" or "Defendant"), and allege the following based upon personal knowledge with respect to Plaintiffs and otherwise on information and belief derived from, among other things, investigation of counsel and review of public documents.

INTRODUCTION

1. This class action lawsuit arises out of a data breach at over 950 Arby's

restaurants located throughout the United States owned and operated by ARG. Many retail stores and fast-food chains have experienced massive data breaches over the past four years, including Target, Home Depot, and Wendy's restaurants, via malicious software installed remotely on point-of-sale ("POS") systems. POS systems and devices are used for managing customer payment transactions, including payments made with debit and credit cards.

2. The susceptibility of POS systems to malware is well-known throughout the retail and restaurant industries. Intruders looking to steal consumer payment card information have targeted POS systems since at least 2005. In the last five years, malware placed on POS systems caused practically every major data breach involving retail stores or fast-food chains, and resulted in millions of compromised payment cards. Data security experts have warned companies like ARG, "[y]our POS system is being targeted by hackers. This is a fact of 21st-century business."[1]

3. Despite the susceptibility of POS systems to hacking, a data breach that compromises sensitive payment card information is not an inevitability of doing business; rather, numerous measures can be taken to prevent intrusion by

[1] *Point of Sale Security: Retail Data Breaches At a Glance*, Datacap Systems, Inc. (May 12, 2016), https://www.datacapsystems.com/blog/point-of-sale-security-retail-data-breaches-at-a-glance#.

unauthorized personnel into POS devices and networks and to limit the effect of an intrusion if it occurs. For example, one data security expert recommends a "Tripod of POS Security," comprised of the following protective measures: (1) POS systems that support EMV chip-based payment cards (a highly secure method of transmitting credit card data that replaces the traditional magnetic stripe); (2) end-to-end encryption, which encrypts payment card data as soon as payment cards are swiped; and, (3) tokenization, which replaces credit and debit card numbers with meaningless series of letters and numbers, rendering any information collected by hackers meaningless.[2]

4. The FTC has also issued guidance and other resources designed to inform businesses of the best practices in data security and to encourage businesses to prioritize data security. Similarly, the leaders of the payment card industry (Visa, MasterCard, Discover, and American Express) have issued specific standards mandating merchants who accept payment cards to meet certain minimum data security requirements. These protections are specifically designed to assist businesses in preventing and limiting data breaches.

5. Given the highly publicized data breaches occurring over the past several years, ARG fully knew of the consequences of a data breach, the

[2] *Id.*

susceptibility of POS systems, and the available measures to enhance data security. Yet, in or around October 2016, computer hackers infiltrated ARG's POS data systems via malicious software at its corporate-owned Arby's restaurants after ARG failed to adequately secure its POS system.[3]

6. For a period of approximately three months (from October 2016 to January 2017), ARG failed to notice that its POS systems at nearly 1,000 Arby's restaurants were infected with malware. When ARG finally learned of the breach in January, it made no immediate public announcement and provided no information to financial institutions that issued compromised payment cards. In fact, the breach became public only after Brian Krebs, a data security investigator, reported on his blog, KrebsOnSecurity.com, that ARG had suffered a data breach via malware placed on Arby's restaurants' POS systems.[4] In February 2017, ARG finally acknowledged that its systems had been breached, compromising payment card information.[5]

7. In April 2017, nearly three months after the data breached ended, and six months after it began, ARG disclosed the extent of its massive data breach:

[3] Brian Krebs, *Fast Food Chain Arby's Acknowledges Breach*, KrebsOnSecurity (Feb. 17, 2017), https://krebsonsecurity.com/2017/02/fast-food-chain-arbys-acknowledges-breach/.

[4] *Id.*

[5] *Security*, Arbys.com (last visited, May 15, 2017), http://arbys.com/security/.

over 950 restaurants infected with malware for an average of 73 days, with some restaurants infected for more than three months. The estimated number of compromised credit and debit cards from one payment card processor alone was over 355,000, making the total breach likely in the tens of millions. This number will likely continue to grow. Some financial institutions have had more payment cards compromised in the Arby's data breach than in any other single breach.

8. The Arby's data breach was the inevitable result of ARG's inadequate data security measures. Despite the well-publicized and ever-growing threat of data breaches involving payment card networks and systems, ARG failed to maintain adequate security measures that could have detected and would have prevented the data breach. ARG also failed to implement data security measures that would have limited the effect of a breach on the financial institutions that issued the payment cards.

9. In addition, ARG exacerbated the injuries suffered by Plaintiffs and the Class by failing to provide notice of the infiltration when it supposedly learned of the breach in January. If Arby's had promptly notified the public of the data breach, the resulting losses would have been less.

10. Had Arby's implemented reasonable data security processes and procedures—measures known and recommended by the payment card industry, the

Federal Trade Commission, and data security experts—ARG would have prevented the breach of its systems, and the extent of the harm caused.

11. The Arby's data breach forced Plaintiffs and other financial institutions to: (a) cancel or reissue compromised credit and debit cards; (b) issue refunds or credits to cover the cost of fraudulent transactions involving compromised cards and accounts; (c) close deposit, transaction, checking, and other compromised accounts, including, but not limited to, stopping payments or blocking transactions with respect to the accounts; (d) reopen deposit, transaction, checking, or other compromised accounts; (e) respond to a significant volume of cardholder complaints, confusion, and concern; and (f) increase fraud monitoring efforts.

12. In addition to the expenses incurred as a result of the data breach, Plaintiffs and the Class also suffered lost revenue in their payment card business as a result of decreased card usage stemming from the data breach.

13. The injuries to Plaintiffs and the Class were directly and proximately caused by ARG's failure to implement and maintain adequate data security measures necessary for protecting customer information, including credit and debit card data and personal identifying information.

14. This class action is brought on behalf of payment card-issuing financial institutions throughout the U.S. to recover the costs that they and others similarly situated have been forced to bear as a direct result of the Arby's data breach. Plaintiffs assert claims for negligence, negligence per se, and declaratory and injunctive relief.

JURISDICTION AND VENUE

15. This Court has original jurisdiction of this Action pursuant to the Class Action Fairness Act, 28 U.S.C § 1332(d)(2). The matter in controversy, exclusive of interest and costs, exceeds the sum or value of $5,000,000 and at least some members of the proposed Class have a different citizenship from ARG.

16. This Court has personal jurisdiction over ARG because Defendant maintains its principal place of business in Georgia, regularly conducts business in Georgia, and has sufficient minimum contacts in Georgia. ARG intentionally availed itself of this jurisdiction by accepting and processing payments for its foods and other services within Georgia.

17. Venue is proper under 18 U.S.C. § 1391(a) because ARG's principal place of business is in this District and a substantial part of the events, acts, and omissions giving rise to Plaintiffs' claims occurred in this District. Venue also lies in the Atlanta division.

PARTIES

18. Each of the Plaintiffs issued payment cards to customers that were compromised by the Arby's data breach and suffered, and continue to suffer, financial injury as described herein. Plaintiffs have also lost interest and transaction fees due to reduced card usage.

19. Plaintiff Fort McClellan Credit Union is an Alabama-chartered credit union, established in 1953, which operates exclusively in northern Alabama. Fort McClellan Credit Union has five branches in Alabama located in Anniston, Roanoke, Jacksonville, Ohatchee, and Centre. Fort McClellan Credit Union issues VISA payment cards and has suffered financial loss due to the Arby's data breach.

20. Plaintiff Midwest America Federal Credit Union is a credit union headquartered in Fort Wayne, Indiana. Midwest America Federal Credit Union is a Visa payment card issuer and has suffered financial loss due to the Arby's data breach.

21. Plaintiff Gulf Coast Bank & Trust Company ("GCBTC") is a bank whose main offices are located in New Orleans, Louisiana. Gulf Coast Bank & Trust Company is a Visa and MasterCard payment card issuer and has suffered financial loss due to the Arby's data breach.

22. Plaintiff Wanigas Credit Union ("Wanigas") is a credit union headquartered in Saginaw, Michigan. Wanigas has over 26,000 members and more than $323 million in assets. Wanigas is a Visa and MasterCard payment card issuer and has suffered financial loss due to the Arby's data breach.

23. Plaintiff Valley Federal Credit Union ("Valley Federal") is a federally chartered credit union with assets of approximately $211 million. Valley Federal is headquartered in Montana and has branches in Montana and Wyoming. Valley Federal is a Visa payment card issuer and has suffered financial loss due to the Arby's data breach.

24. Defendant Arby's Restaurant Group, Inc. is incorporated in Delaware and operates its principal place of business in Atlanta, Georgia. ARG accepts payment cards issued by Plaintiffs and the Class to pay for goods and services at its Arby's restaurants, and processes the payments through its POS network.

STATEMENT OF FACTS

25. ARG operates Arby's restaurants, a fast-food chain restaurant specializing in roast beef and other protein-based sandwiches. The first Arby's restaurant opened in 1964 and since then, Arby's has expanded to nearly 3,300 stores globally, including 1,000 restaurants owned and operated by ARG (those at issue in this breach) and several thousand stores operating under a franchisee

license.

26. Arby's restaurants have proved to be quite profitable, raking in annual sales of approximately $1.12 billion in 2015.[6] In the first quarter of 2016, Arby's posted 5.8% U.S. same-store sales growth, the twenty-second consecutive quarter Arby's has seen growth in that sector and the thirteenth straight quarter of outperforming the industry as a whole.[7]

27. With its growing profitability, ARG has heavily invested in remodeling its restaurants. In 2014, ARG launched its "Inspire Design" restaurant, a remodeling effort which ARG claims has boosted sales by 15% at remodeled restaurants.[8] In 2015, nearly 200 of Arby's 3,300 locations were remodeled and upgraded to fit their new brand with plans to continue to remodel restaurants in 2016 and beyond.[9]

28. Despite ARG's substantial investments made to modernize its branding and upgrade the appearance of its restaurants, ARG failed to make meaningful improvements to the security of its POS systems and administrative

---

[6] Beth Kowitt, *How Arby's (Yes, Arby's) Is Crushing It*, Fortune (Apr. 27, 2016), http://fortune.com/2016/04/27/arbys-sales-growth/.

[7] *Id.*

[8] *Brand Milestones*, Arbys.com (last visited, Feb. 28, 2018), http://arbysfranchising.com/research/brand-milestones/.

[9] Kowitt, *supra* note 6.

network, placing the purchasing information of its customers at risk. From October 2016 to January 2017, ARG's lax data security allowed intruders to place malware on POS devices in more than 950 corporate-owned restaurants, exposing sensitive payment card information on millions of credit and debit cards.

Background on Data Breaches Involving Malware on Company POS Systems

29. A wave of data breaches causing the theft of retail payment card information has hit the United States in the last several years.[10] In 2016, the number of U.S. data breaches surpassed 1,000, a record high and a forty percent increase in the number of data breaches from the previous year.[11] The amount of payment card data compromised by data breaches is massive. For example, in 2013 and 2014 it is estimated that over 100 million cards were compromised.[12]

30. Most of the massive data breaches occurring within the last several years involved malware placed on POS systems used by merchants. For example, in 2013, hackers infiltrated Target, Inc.'s POS system, stealing information from

[10] *Data Breaches Increase 40 Percent in 2016, Finds New Report From Identity Theft Resource Center and CyberScourt*, Identity Theft Resource Center (Jan. 19, 2017), http://www.idtheftcenter.org/2016data-breaches.html.

[11] *Id.*

[12] Symantec, *A Special Report On Attacks On Point-of-Sale Systems* 3 (Nov. 20, 2014), https://www.symantec.com/content/dam/symantec/docs/white-papers/attacks-on-point-of-sale-systems-en.pdf

an estimated 40 million payment cards in the United States.[13] In 2014, over 7,500 self-checkout POS terminals at Home Depots throughout the United States were hacked, compromising roughly 56 million debit and credit cards.[14] In 2016, on-site POS systems at more than 1,000 Wendy's restaurants were infiltrated with malware, resulting in the theft of payment cards data for nearly six-months.[15]

31. A POS system is an on-site device which manages transactions from consumer purchases, both by cash and card. When a payment card is used at a POS terminal, "data contained in the card's magnetic stripe is read and then passed through a variety of systems and networks before reaching the retailer's payment processor."[16] The payment processor then passes on the payment information to the financial institution that issued the card and takes the other steps needed to complete the transaction.[17]

---

[13] Krebs, *supra* note 3.

[14] Brett Hawkins, *Case Study: The Home Depot Data Breach* 7 (SANS Institute, Jan. 2015), https://www.sans.org/reading-room/whitepapers/casestudies/case-study-home-depot-data-breach-36367.

[15] Krebs, *supra* note 3.

[16] Symantec, *supra* note 12, at 6.

[17] Salva Gomzin, Hacking Point of Sale: Payment Application Secrets, Threats, and Solutions 8 (Wiley 2011).

32. The flow of information from input to payment processing is called the POS deployment architecture.[18] Most retailers use one of five architectures to process in-store transactions.[19] Unless adequate security measures are implemented, each type of deployment architecture is vulnerable to data theft because multiple devices and networks must, at some point, store payment card data as it is transferred to the payment processor.[20] The risk increases with the number of devices and systems used to complete the data transfer and the amount of connectivity as well as the number entities with access to the payment processing network.

33. Before transmitting customer data over the merchant's network through the deployment architecture, POS systems typically, and very briefly, store the data in plain text within the system's memory.[21] The stored information includes "Track 1" and "Track 2" data from the magnetic strip on the payment card, such as the cardholder's first and last name, the expiration date of the card, and the CVV (three number security code on the card).[22] This information is

[18] *Id.* at 39.

[19] *Id.* at 43-50.

[20] *Id.*

[21] Symantec, *supra* note 12, at 6.

[22] Gomzin, *supra* note 17, at 98-101.

unencrypted on the card and, at least briefly, will be unencrypted in the POS terminal's temporary memory as it processes the data.[23]

34. Intruders seek to obtain access to the unencrypted information on the POS system. In ordered to directly access a POS device, hackers generally follow four steps: infiltration, propagation, exfiltration and aggregation.[24] In the infiltration phase, an "attacker gains access to the target environment"[25] allowing the hackers to move through a business's computer network, find an entry point into the area that handles consumer payments, and directly access the physical POS machines at in-store locations.[26] This often occurs through a "phishing" email to an outside vendor.

35. The attacker then infects or propagates the POS systems with malware.[27] The malware "collects the desired information . . . and then exfiltrates the data to another system" called the "aggregation point."[28]

---

[23] Symantec, *supra* note 12, at 5.

[24] *Point of Sale Systems and Security: Executive Summary*, SANS Institute 4 (Oct. 2014), https://www.sans.org/reading-room/whitepapers/analyst/point-sale-systems-security-executive-summary-35622.

[25] *Id.*

[26] Symantec, *supra* note 1, at 6.

[27] SANS, *supra* note 24, at 4.

[28] *Id.*

36. From the aggregation point, payment data is transferred to a system outside the target environment, where it can usually be retrieved without detection. A diagram depicting the way in which the hackers operate follows:

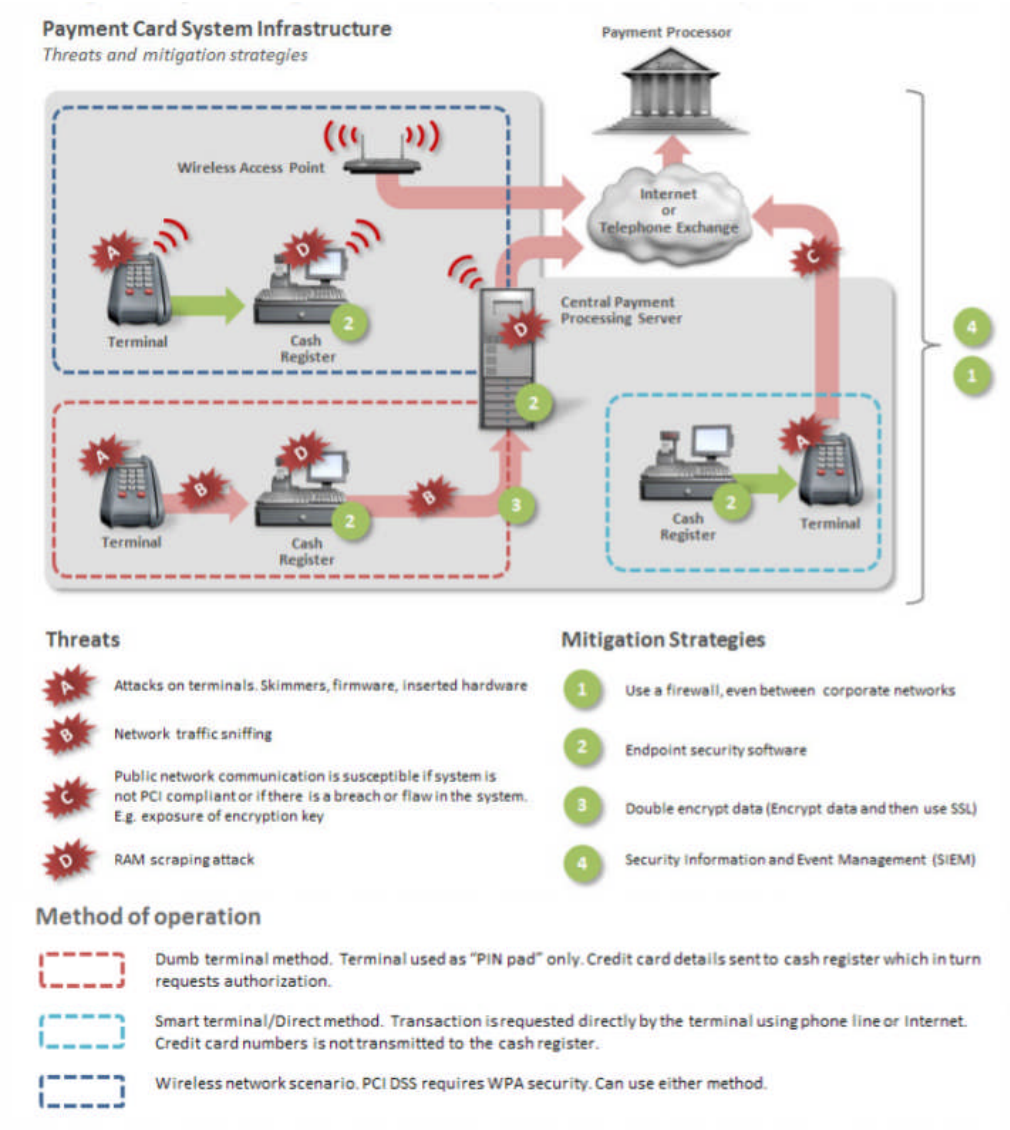

Figure 1. **An example of a POS deployment architecture and its vulnerabilities.**

37. Intruders with access to Track 1 and Track 2 payment card data can physically replicate the card or use it online. Unsurprisingly, theft of payment card information via POS systems is now "one of the biggest sources of stolen payment cards."[29] Since 2014, malware installed by POS has been responsible for nearly every major data breach of a retail outlet or restaurant.[30]

ARG Was On-Notice of the Susceptibility of POS Devices and the Consequences of a Breach

38. ARG knew or should have known of the susceptibility of its POS systems and that a breach of its corporate network would permit intruders to install malware at its locations throughout the U.S., putting millions of debit and credit cards issued by Plaintiffs and the Class at risk.

39. In 2015, intrusions into POS systems accounted for 64% of all breaches where intruders successfully stole data.[31] A 2016 report by Verizon confirmed "[t]he vast majority of successful breaches leverage legitimate credentials to gain access to the POS environment. Once attackers gain access to the POS devices, they install malware, usually a RAM scraper, to capture payment

[29] Symantec, *supra* note 12, at 3.

[30] *See, e.g.*, *2016 Data Breach Investigations Report*, Verizon at 1 (Apr. 2016), http://www.verizonenterprise.com/resources/reports/rp_2016-DBIR-Retail-Data-Security_en_xg.pdf.

[31] *Id.* at 3.

card data."[32] According to Verizon, hackers successfully compromise POS systems in a matter of minutes or hours and exfiltrate data within days of placing malware on the POS devices.[33]

40. Given the numerous reports indicating the susceptibility of POS systems and consequences of a breach, as reported by Verizon and other media outlets, ARG knew or should have known of the need to safeguard its POS systems.

41. ARG was also put on notice of the need for adequate data security measures by the well-publicized data breaches that occurred at other retail stores and restaurants, including those at Neiman Marcus, Michaels, Sally Beauty Supply, P.F. Chang's China Bistro, Goodwill, SuperValu Grocery, UPS, Home Depot, Jimmy John's, Dairy Queen, Staples, Kmart, Wendy's, Noodles & Co., Eddie Bauer, and GameStop.

42. Just last year, the risk of a massive data breach was highlighted for ARG once again by the data breach at another fast food chain. Wendy's Restaurants' POS systems were compromised by malware which stole payment card information for over a half-year period. Hackers gained entry into Wendy's

[32] *Id.*

[33] *Id.* at 4.

POS machines through similar methods used in the Target breach: compromised credentials provided to vendors with remote access to Wendy's network.[34] Once hackers had access to Wendy's corporate network, they deployed malware onto POS terminals at franchisee locations, which ultimately collected payment card data.[35] At least one security expert believed EMV chip readers at franchisee locations would have prevented some theft of payment data.[36]

43. The data breach at Wendy's should have been a major red flag for ARG, not only because Wendy's operated a similar fast food chain but also because between 2008 and 2011, ARG and Wendy's International were corporate affiliates through a merger, which created the Wendy's/Arby's Group, Inc. Before the two fast food chains separated, the group purchased POS terminals for both Wendy's in 2009[37] and Arby's in 2010.[38] Wendy's/Arby's Group installed POS

---

[34] *Wendy's Update on Payment Card Security Incident*, Wendys.com (last visited, Apr. 26, 2017), http://ir.wendys.com/phoenix.zhtml?c=67548&p=irol-newsArticle&ID=2182670

[35] *Id.*

[36] Brian Krebs, *1,025 Wendy's Locations Hit in Card Breach*, KrebsOnSecurity (July, 16, 2016), https://krebsonsecurity.com/2016/07/1025-wendys-locations-hit-in-card-breach/#more-35408.

[37] *Fast-Food Chain to Deploy NCR Payment Terminals*, NCR Corp. (Dec. 8, 2009), https://www.paymentsource.com/news/fast-food-chain-to-deploy-ncr-payment-terminals.

software suites, including Aloha Enterprise Suite, Aloha Quick Service POS, Aloha Command Center, Aloha Configuration Center, Aloha Insight, and both Radiant POS terminals and NCR POS terminals.[39] Upon information and belief, Wendy's and Arby's used similar POS systems.

44. In fact, Wendy's shareholders have claimed the "point-of-sale system . . . was fraught with vulnerabilities" and the company failed "to implement or enforce any effective internal data security procedures."[40] ARG knew or should have known of the weakness of Wendy's data security measures, particularly to the extent that ARG used the same systems.

45. Despite the vulnerabilities of POS systems, available security measures and businesses practices would have significantly reduced or eliminated the likelihood that hackers could successfully infiltrate business' POS systems. The payment card networks (MasterCard, VISA, Discover, and American Express), data security organizations, state governments, and federal agencies have

---

[38] *Arby's Deploys Radiant's Aloha POS Solution*, QSR Web (Jan. 6, 2010), https://www.qsrweb.com/news/arbys-deploys-radiants-aloha-pos-solution-2/.

[39] *Id.*

[40] Steven Trader, *Wendy's hit With Shareholder Suit Over Customer Data Breach*, Law360 (Dec. 16, 2016), https://www.law360.com/articles/873987/wendy-s-hit-with-shareholder-suit-over-customer-data-breach.

all implemented various standards and guidance on security measures designed to prevent these types of intrusions into POS systems.

46. ARG's adherence to guidance and standards suggested by data security organizations and federal agencies, as well as those mandated by the payment card networks, would have prevented this data breach. One report indicated that over 90% of the data breaches occurring in 2014 were preventable.[41] Further, another report noted that businesses that fail to take adequate and available security measures, such as by allowing their "point-of-sale system [to be] fraught with vulnerabilities" and lacking "effective internal data security procedures, are at serious risk of a breach."[42]

47. In this case, despite Defendant's understanding of the risk of data theft via malware installed on its POS systems and the widely available resources to prevent intrusion into its POS data systems, Defendant failed to take reasonable and sufficient protective measures.

Arby's Restaurant Group, Inc. is Breached Via Its POS System, Allowing the Theft of Payment Card Information

48. ARG is, and at all relevant times was, aware that the payment card data it maintains via credit and debit card transactions is highly sensitive and could

[41] Verizon, *supra* note 30, at 1.

[42] Trader, *supra* note 40.

be used for nefarious purposes by third parties, such as perpetrating identity theft and making fraudulent purchases. ARG knew of the necessity of safeguarding its customers' payment card data and of the foreseeable consequence that would occur if its data security systems were breached, including the significant costs that would be imposed on issuers, such as Plaintiffs, members of the Class, and others. Other retail and fast-food chain data breaches put ARG on notice of the means by which intruders infiltrate POS systems and obtain payment card data.

49. ARG is, and at all relevant times was, fully aware of the significant volume of daily credit and debit card transactions at Arby's restaurants, amounting to tens of thousands of daily credit card transactions, and thus, the significant number of individuals who would be harmed by a breach of ARG's POS systems.

50. Despite the well-known susceptibility of POS systems and the highly publicized complications caused by data breaches – including those at similar fast food chains like Wendy's and Noodles & Co. – ARG failed to implement necessary data protocols to prevent a data breach.

51. In October 2016, intruders gained access to ARG's corporate network and eventually placed malware on POS systems at over 950 Arby's restaurants in

the United States.[43]

52. An early indication of a massive data breach for financial institutions occurs when payment card networks issue alerts, including the Compromised Account Management System Alerts ("CAMS") from VISA, and Account Data Compromise Alerts ("ADC") from MasterCard. These alerts list specific payment card accounts believed to be compromised in a data breach tied to a specific retailer. The number of compromised accounts listed in CAMS and ADC alerts related to the Arby's data breach were among the largest number of alerts ever received for a single event. This is "generally a sign of a sizeable nationwide breach."[44]

53. After receiving "long lists of compromised cards from both VISA and MasterCard," the PSCU – a Credit Union Service Organization that serves over 800 credit unions – sent out an alert to member credit unions.[45] The alert indicated that Track 1 and Track 2 data may have been compromised by the breach, meaning cardholder names, primary account numbers, expiration dates, and in some cases, PIN numbers were all stolen. The length of exposure, or the "exposure window,"

[43] To determine the number of stores, information was gathered from ARG's breached restaurant locations. *See Security - Locations*, Arbys.com (last visited, May 15, 2017), http://arbys.com/security/.

[44] Krebs, *supra* note 3.

[45] *Id.*

was an estimated three month period between October 25, 2016 and January 19, 2017; however, Arby's later revealed the breach lasted even longer.

54. Eventually, financial institutions traced the alerts issued for their customers' accounts and found the ubiquitous transaction: purchases at Arby's restaurants.

55. The breach became public on February 9, 2017 through an article published by Brian Krebs of KrebsOnSecruity, a leading information security investigator.[46] KrebsOnSecurity announced that it reached out to ARG after hearing from several financial institutions about a suspected data breach at Arby's restaurants. In response to Krebs's inquiry, an ARG representative confirmed that Arby's recently remediated a breach involving malicious software installed on payment card systems at hundreds of its restaurant locations nationwide.[47]

56. According to Krebs, a spokesperson for ARG said that Defendant was first notified by industry partners in mid-January about a breach at some of its locations. ARG indicated that the breach involved malware placed on payment systems inside Arby's corporate stores, although Arby's claims that not all of its 1,000 corporate-owned restaurants were impacted.

[46] *See* Krebs, *supra* note 3.

[47] *Id.*

57. Eventually, Arby's made an official public announcement, admitting its systems had been breached. The announcement came approximately four months after the breach began and one month after it was resolved. ARG, however, failed to provide any additional about the scope and extent of the breach. The announcement in full was:

> Arby's Restaurant Group, Inc. (ARG) was recently provided with information that prompted it to launch an investigation of its payment card systems. ARG immediately notified law enforcement and enlisted the expertise of leading security experts, including Mandiant. While the investigation is ongoing, ARG quickly took measures to contain this incident and eradicate the malware from systems at restaurants that were impacted. ARG reminds guests that it is always advisable to closely monitor their payment card account statements for any unauthorized activity. If guests discover any unauthorized charges, they should report them immediately to the bank that issued their card.

58. In its announcement, ARG failed to take responsibility for the breach of its POS system. Instead, it put the onus on consumers and the card-issuing financial institutions to identify and resolve any fallout by stating, "ARG reminds guests that it is always advisable to closely monitor their payment card account statements for any unauthorized activity. If guests discover any unauthorized charges, they should report them immediately to the bank that issued their card."

59. In March, ARG provided an updated notice.[48] As expected, ARG admitted the data breach was a result of malware placed on its POS systems, allowing intruders to access and obtain payment card data (as has occurred in nearly every major retail and fast-food chain data breach.)

60. ARG did not indicate and still has not indicated how its corporate network was breached by hackers. However, there are two fundamental ways a hacker could have accessed Arby's systems: (1) by exploiting the credentials of an ARG vendor; or (2) by accessing ARG's systems directly. In either case, the data breach could not have happened but for ARG's failure to satisfy its duty to exercise reasonable care.

61. If intruders exploited an ARG service provider's limited corporate credentials, then ARG's corporate network was invaded in the exact same manner as Target and Wendy's, which is logical since ARG and Wendy's were corporate siblings until recently. Not only is an intrusion into a corporate network via a third-party service provider's limited credentials preventable, ARG should have known hackers would seek to exploit such credentials because they did so in previous data breaches.

[48] *See* Arby's.com, *supra* note 43.

62. If, in fact, the hackers did not enter using a service provider's credentials, they entered directly into ARG's system and were able to do so because ARG lacked sufficient corporate IT security measures. The failure to protect its own network from direct attack by hackers is even more egregious than the failure to police the security practices of its service providers.

63. ARG's updated notice also sheds light on the massive scale of the breach. According to the location data provided by ARG – which includes the state, city and zip code of the compromised restaurant and the breach start date and end date[49] – malware was placed on 956 corporate-owned Arby's restaurants. The infiltrated restaurants are located in 24 states and 648 cities throughout the United States.

64. Although ARG initially indicated the breach began "no earlier than October 20, 2016" its updated notice indicates that as of October 12, 2016, intruders had placed malware on POS devices at 53 Arby's restaurants and by the end of October, intruders compromised POS devices at another 849 restaurants. The average length of time the data collecting malware was installed was over 73 days, while over 50 restaurants were compromised for more than 90 days.[50]

[49] *Id.*

[50] *Id.*

65. Intruders, therefore, had months to collect payment card data unabated. During this time, Arby's failed to recognize its systems had been breached and that intruders were stealing data on millions of payment cards. By comparison, Target recognized and resolved its data breach in approximately 16 days. Quick action by ARG likely would have significantly reduced the consequences of the breach. Instead, ARG took more than three months to realize its systems had been breached, and thus contributed to its scale.

66. Plaintiffs and the Class were required to act immediately to mitigate the fraudulent transactions being made on payment cards that they had issued, while simultaneously taking steps to prevent future fraud. Consumers are ultimately protected from most fraud loss, but Plaintiffs and class members are not. By regulation, financial institutions bear primary responsibility for reimbursing consumers for fraudulent charges on the payment cards they issue.

ARG Failed to Implement Data Security Protocols Recommended by Federal Agencies, Security Experts, and the Payment Card Industry

67. Security experts have recommended specific steps that retailers should take to protect their POS systems. For example, more than two years ago, Symantec recommended "point to point encryption" implemented through secure card readers, which encrypts credit card information in the POS system, preventing "RAM-scraping" malware that extracts card information through the POS memory

while it processes the transaction. Symantec also highlighted the need to utilize updated software to avoid susceptibility in older operating systems being phased out, like Windows XP or Windows XP Embedded. Moreover, Symantec emphasized the importance of adopting EMV chip technology. Last year, Datacap Systems recommended similar preventative measures.[51]

68. The major payment card industry brands (MasterCard, VISA, Discover, JCB, and American Express) set forth significant and specific security measures in their Card (or sometimes, Merchant) Operating Regulations. Card Operating Regulations are binding on merchants and require merchants to: (1) protect cardholder data and prevent its unauthorized disclosure; (2) store data, even in encrypted form, no longer than necessary to process the transaction; and (3) comply with all industry standards.

69. The payment card industry, like Symantec and DataSystems, has also strongly encouraged the use of POS terminals capable of accepting payment from EMV chips. EMV chip technology uses embedded computer chips instead of magnetic stripes to store payment card data. Unlike magnetic-stripe cards that use static data (the card information never changes), EMV cards use dynamic data. Every time an EMV card is used, the chip creates a unique transaction code that

[51] *See* Datacap Systems, *supra* note 1.

cannot be used again. Such technology greatly increases security because if an EMV chip's information is stolen, the unique number cannot be used by the hackers, making it much more difficult for criminals to profit from what is stolen.

70. The Payment Card Industry ("PCI") Council informed retailers such as ARG that: "Card brands expect merchants' POS terminals and software to be EMV-capable by October 1, 2015."[52] Additionally, Card Operating Regulations shifted liability for card-present fraudulent transactions to those merchants who failed to install POS devices capable of receiving cards with EMV chips by October 1, 2015.[53]

71. The PCI Security Standards Council promulgates data security standards (referred to as "PCI DSS") to "encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures." PCI DSS applies "to all entities involved in payment card processing—including merchants, processors, acquirers, issuers, and service providers. PCI DSS comprises "a minimum set of requirements for protecting data."

---

[52] PCI Security Standards Council, *Merchant Guide: Stepping Up to EMV Chip With PCI* (2015), https://www.pcisecuritystandards.org/pdfs/Merchant_Guide_-_Stepping_Up_to_EMV_Chip_with_PCI_-v06.pdf.

[53] EMV Migration Forum, *Understanding the 2015 U.S. Fraud Liability Shifts* (May 2015), http://www.emv-connection.com/downloads/2015/05/EMF-Liability-Shift-Document-FINAL5-052715.pdf.

72. PCI DSS 3.1, the version of the standards in effect at the time of the data breach, sets forth detailed and comprehensive requirements that must be followed to meet each of the following twelve "high-level" mandates:

PCI Data Security Standard – High Level Overview

Build and Maintain a Secure Network and Systems	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Identify and authenticate access to system components 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel

73. Among other things, PCI DSS required Defendant to: (1) properly secure payment card data; (2) not store cardholder data beyond the time necessary to authorize a transaction; (3) maintain up-to-date antivirus software and a proper firewall; (4) restrict access to payment card data on a need-to-know basis; (5) establish a process to identify and timely fix security vulnerabilities; (6) assign unique identification numbers to each individual with access to its systems; and (7) encrypt payment card data at the point of sale.

74. Compliance by retailers with PCI DSS is required, but PCI DSS only sets forth the minimum protective action a business must take. Even in 2014, security experts recognized that "[w]hile PCI-DSS provides a framework for improved payment processing, it is clear that it has been insufficient to ensure the security of modern retail POS systems. To truly improve the security posture of POS devices, organizations must take a more dynamic approach."[54] In fact, every company that has been spectacularly hacked in the last three years purportedly has been PCI compliant. Target, Wendy's, Home Depot, Neiman Marcus, Michael's stores, Sally Beauty Holdings, Inc., Supervalu, Albertson's and many other businesses subjected to data breaches were thought to be PCI DSS compliant at the time of the compromise.[55]

75. Federal and State governments have likewise established security standards and issued recommendations to temper data breaches and the resulting harm to consumers and financial institutions. The Federal Trade Commission ("FTC") has issued numerous guides for business highlighting the importance of reasonable data security practices. According to the FTC, the need for data

[54] SANS, *supra* note 24, at 1.

[55] *Id.*

security should be factored into all business decision-making.[56] The FTC's recommended security measures include encrypting information stored on computer networks; holding on to information only as long as necessary; properly disposing of personal information that is no longer needed; limiting administrative access to business systems; using industry-tested and accepted security methods; monitoring network activity to uncover unapproved activity; verifying that privacy and security features work; testing for common vulnerabilities; and, updating and patching third-party software.[57]

76. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

---

[56] Federal Trade Comm'n, *Start With Security A Guide For Business, Lessons Learned from FTC Cases* (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

[57] *See id;* Federal Trade Comm'n, *Protecting Personal Information, A Guide For Business* (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

77. Several states have specifically enacted data breach statutes requiring merchants to use reasonable care to guard against unauthorized access to consumer information, such as California Civil Code §1798.81.5(b) and Wash. Rev. Code §19.255, or that otherwise impose data security obligations on merchants, such as Minnesota Plastic Card Security Act, Minn. Stat. §325E.64. Most states have also enacted statutes requiring merchants to provide notice to consumers of security systems breaches. These statutes, implicitly or explicitly, mandate the use of reasonable data security practices and reflect the public policy of protecting sensitive customer data.

78. In this case, ARG was at all times fully aware of its obligation to protect the financial data of its customers because of its participation in payment card processing networks. ARG was also aware of the significant repercussions if it failed to do so because it collected payment card data from tens of thousands of customers daily and knew that this data, if hacked, would damage the financial institutions that issued the cards.

79. Despite understanding the consequences of inadequate data security, ARG failed to comply with PCI DSS requirements; failed to take additional protective measures beyond those required by PCI DSS; failed to implement EMV-capable POS systems by the October 1, 2015 deadline; operated POS systems with

outdated operating systems and software; failed to enable point-to-point and end-to-end encryption; and, failed to take other measures necessary to protect its corporate network.

80. The Arby's data breach was a direct result of ARG's failures. ARG failed to reasonably protect cardholder information, putting consumer financial accounts in jeopardy and forcing financial institutions, like Plaintiffs and the Class, to take remedial action for ARG's inadequate preventative security measures.

81. ARG had the resources to prevent a breach, having spent substantial funds to remodel and upgrade its restaurants throughout the United States with its "Inspire Design" image. Additionally, since 2013, ARG has dramatically increased the profitability of Arby's restaurants and its overall annual gross profits. ARG made significant expenditures to market its products; modernize its restaurants; add menu items; and, revitalize its brand. Nonetheless, ARG neglected to adequately invest in data security, despite the growing number of POS intrusions and several years of well-publicized data breaches.

82. Had ARG remedied the deficiencies in its POS systems, followed PCI DSS guidelines, and adopted security measures recommended by experts in the field, ARG would have prevented intrusion into its POS systems and, ultimately, the theft of its customers' confidential payment card information.

83. Because ARG failed to take reasonable protective measures to prevent a data breach, Plaintiffs and the Class have been and will continue to be required to bear the costs of preventing and repaying fraudulent transactions made with credit and debit card information obtained through ARG's POS systems.

CLASS ALLEGATIONS

84. Plaintiffs bring this action on behalf of themselves and all other similarly situated Class members pursuant to Rule 23(a), (b)(2) and (b)(3) of the Federal Rules of Civil Procedure and seek certification of the following Nationwide Class:

> All banks, credit unions, financial institutions, and other entities in the United States (including its Territories and the District of Columbia) that issued payment cards (including debit or credit cards) used by consumers to make purchases at Arby's restaurants during the period from October 8, 2016 to January 12, 2017.

85. Excluded from the Class are Defendant and its subsidiaries and affiliates; all employees of Defendant; all persons who make a timely election to be excluded from the Class; government entities; and the judge to whom this case is assigned and her immediate family and court staff.

86. Plaintiffs reserve the right to modify, expand or amend the above class definition or to seek certification of a class or subclasses defined differently than

above before any court determines whether certification is appropriate following discovery.

87. **Numerosity.** Consistent with Rule 23(a)(1), the Class are so numerous and geographically dispersed that joinder of all Class members is impracticable. Plaintiffs believe that there are thousands of members of the Class and the sheer number of accounts alerted-on by payment card networks indicates the Class is numerous. Class members may be identified through objective means. Class members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods, which may include U.S. mail, electronic mail, internet postings, and/or published notice.

88. **Commonality and Predominance.** Consistent with Fed. R. Civ. P. 23(a)(2) and with 23(b)(3)'s predominance requirement, this action involves common questions of law and fact that predominate over any questions affecting individual Class members. These common questions include, without limitation:

a. Whether ARG knew or should have known of the susceptibility of its POS systems to a data breach;

b. Whether ARG's security measures to protect is POS systems were reasonable in light of the PCI DSS requirements, FTC data security recommendations, and other measures recommended by data security experts;

c. Whether ARG's failure to adequately comply with PCI DSS standards and/or to institute protective measures beyond PCI DSS standards amounted to negligence;

d. Whether ARG's failure to implement adequate data security measures allowed the breach of its POS data systems to occur;

e. Whether reasonable security measures known and recommended by the data security community could have reasonably prevented the breach of ARG's POS systems;

f. Whether reasonable measures to monitor and detect unauthorized activity known and recommended by the data security community could have stymied the data breach in less than three months;

g. Whether adherence to PCI DSS requirements, FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the breach of the POS systems;

h. Whether Plaintiffs and the Class were injured and suffered damages or other acceptable losses because of ARG's failure to reasonably protects its POS data systems and corporate network;

i. Whether Plaintiffs and the Class are entitled to relief;

89. **Typicality.** Consistent with Fed. R. Civ. P. 23(a)(3), Plaintiffs are typical members of the Class. Plaintiffs are financial institutions that issued payment cards compromised by the infiltration and theft of card payment information from ARG's POS system. Plaintiffs' injures are akin to other class members and Plaintiffs seek relief consistent with the relief of the Class.

90. **Adequacy.** Consistent with Fed. R. Civ. P. 23(a)(4), Plaintiffs are adequate representatives of the Class because Plaintiffs are members of the Class and are committed to pursuing this matter against ARG to obtain relief for the Class. Plaintiffs have no conflicts of interest with the Class. Plaintiffs have also retained counsel competent and experienced in complex class action litigation of this type, having previously litigated several data breach cases to successful results on behalf of financial institutions. Plaintiffs intend to vigorously prosecute this case and will fairly and adequately protect the Class' interests.

91. **Superiority.** Consistent with Fed. R. Civ. P 23(b)(3), class action litigation is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The quintessential purpose of the class action mechanism is to permit litigation against wrongdoers even when damages to individual plaintiffs may not be sufficient to justify individual litigation. Here, the damages suffered by Plaintiffs and the Class are relatively small compared to the burden and expense required to individually litigate their claims against Defendant, and thus, individual litigation to redress Defendant's wrongful conduct would be impracticable. Individual litigation by each Class member would also strain the court system. Individual litigation creates the

potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court.

92. **Injunctive and Declaratory Relief.** Consistent with Fed. R. Civ. P. 23(b)(2), Defendant, through its uniform conduct, acted or refused to act on grounds generally applicable to the Class as a whole, making injunctive and declaratory relief appropriate to the Class as a whole.

CHOICE OF LAW

93. Arby's acts and omissions discussed herein were orchestrated and implemented at its corporate headquarters in Georgia and actions (and inactions) complained of occurred in, and radiated from, Georgia.

94. The key wrongdoing at issue (Arby's failure to employ reasonable data security measures) emanated from Arby's headquarters in Georgia.

95. Arby's corporate point-of-sale system and IT personnel operate out of and are located at Arby's headquarters in Georgia. For example, Arby's recently sought a Senior Engineer, Information Security and Compliance position to handle PCI-DSS assessments and other duties at its Atlanta headquarters.

96. Georgia, which seeks to protect the rights and interests of Georgia and other U.S. businesses against a company doing business in Georgia, has a greater interest in the claims of Plaintiffs and the Class members than any other state and is most intimately concerned with the outcome of this litigation.

97. Application of Georgia law to a nationwide Class with respect to Plaintiffs' and the Class members' claims is neither arbitrary nor fundamentally unfair because Georgia has significant contacts and a significant aggregation of contacts that create a state interest in the claims of the Plaintiffs and the nationwide Class.

98. Arby's licensing agreements with franchisees have a governing law provision that directs that Georgia law should apply and that disputes must be resolved in the jurisdiction where Arby's principal office is located (Atlanta, Georgia).

99. The location where Plaintiffs reside was fortuitous and Arby's could not have foreseen where affected payment card issuers would reside, as Arby's didn't know which credit unions and banks Arby's customers used and the location of these financial institutions' headquarters, or principal places of business, at the time of the breach.

100. Further, under Georgia's choice of law principles, which are applicable to this action, the common law of Georgia will apply to the claims of all Class members.

COUNT I

Negligence

101. ARG owed an independent duty to Plaintiffs and the members of the Class to take reasonable care in managing and protecting cardholder information, and to timely notify Plaintiffs in the case of a data breach. This duty arises from multiple sources.

102. ARG owes an independent, general duty of reasonable care to Plaintiffs and the Class because it was foreseeable that ARG's data systems and the cardholder data those data systems processed would be targeted by hackers. It also was foreseeable that such hackers would extract cardholder data from ARG's systems and misuse that information to the detriment of Plaintiffs and the Class, and that Plaintiffs and the Class would be forced to mitigate such fraud (or potential fraud) by reissuing payment cards and reimbursing fraud losses.

103. ARG's common law duty also arises from the special relationship that existed between ARG and the Class. Plaintiffs and the Class entrusted ARG with the cardholder data contained on the payment cards Plaintiffs and the Class issued.

ARG, as the holder and processor of that information, was the only party who realistically could ensure that its data systems were sufficient to protect the data it was entrusted to hold.

104. In addition to the common law, Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45, further mandated Defendant to take reasonable measures to protect the cardholder data. Section 5 prohibits unfair practices in or affecting commerce, which requires and obligates ARG to take reasonable security measures. The FTC publications and data security breach orders described herein further form the basis of ARG's duty to adequately protect sensitive card payment information. In addition, individual states have enacted statutes based upon the FTCA that also created a duty.

105. ARG is also obligated to perform its business operations in accordance with industry standards, including the PCI DSS, to which ARG is bound. The industry standards create yet another source of obligations that mandate ARG exercise reasonable care with respect to Plaintiffs and the Class.

106. ARG, by its actions, has breached its duties to Plaintiffs and the Class. Specifically, ARG failed to act reasonably in protecting payment card data, and did not have reasonably adequate systems, procedures and personnel in place to prevent the disclosure and theft of payment card data.

107. ARG also had the opportunity and resources to prevent a data breach. ARG has increased significantly in profitability and has specifically emphasized remodeling its restaurants. ARG's remodeling efforts could have easily included updated POS systems and updated software to protect its customers' payment card information. ARG was fully aware of the possibility and consequence of a breach of its POS system. Additionally, the FTC, PCI, and other data security experts have proffered guidance and methods to enhance the security of POS data systems and networks. ARG, however, failed to take such action leaving its data systems unreasonably vulnerable to a breach.

108. As a direct and proximate result of ARG's conduct, Plaintiffs and the Class have suffered and continue to suffer injury, including but not limited to cancelling and reissuing payment cards, refunding fraudulent charges, changing or closing accounts, notifying members that their cards were compromised, investigating claims of fraudulent activity, increasing fraud monitoring on potentially impacted accounts, and taking other steps to protect themselves and their members. In addition, the cards they issued (and the corresponding account numbers) were rendered worthless.

109. Because no statutes of other states are implicated, Georgia common law applies to the negligence claims asserted by Plaintiffs and the Class.

COUNT II

Negligence Per Se

110. Section 5 of the Federal Trade Commission Act, 15 U.S.C. §45, prohibits "unfair. . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by retailers, restaurants and other businesses such as ARG of failing to use reasonable measures to protect cardholder data. The FTC publications and orders described herein also form the basis of ARG's duty.

111. ARG violated Section 5 of the FTCA by failing to use reasonable measures to protect cardholder data and by not complying with applicable industry standards, including PCI DSS as described herein. ARG's conduct was particularly unreasonable given the nature and amount of cardholder data it obtained and stored and the foreseeable consequences of a data breach at a national restaurant, including specifically the immense damages that would result to consumers and financial institutions like Plaintiffs and the Class.

112. ARG's violation of Section 5 of the FTCA (and similar state statutes) constitutes negligence per se.

113. Plaintiffs and the Class are within the class of persons Section 5 of the FTCA (and similar state statutes) were intended to protect because they are

engaged in trade and commerce and bear primary responsibility for reimbursing consumers for fraud losses. Moreover, Plaintiffs and many class members are credit unions, which are organized as cooperatives whose members are consumers.

114. Additionally, the harm that has occurred is the type of harm the FTCA (and similar state statutes) were intended to guard against. The FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiffs and the Class.

115. As a direct and proximate result of Defendant's negligence per se, Plaintiffs and the Class have suffered and continue to suffer injury, including but not limited to cancelling and reissuing payment cards, refunding fraudulent charges, changing or closing accounts, notifying members that their cards were compromised, investigating claims of fraudulent activity, increasing fraud monitoring on potentially impacted accounts, and taking other steps to protect themselves and their members. In addition, the cards they issued (and the corresponding account numbers) were rendered worthless.

116. Because no statutes of other states are implicated, Georgia common law applies to Plaintiffs and the Class's negligence per se claim.

COUNT III

Declaratory and Injunctive Relief

117. Under the Declaratory Judgment Act, 28 U.S.C. §§2201, et seq., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, which are tortious and which violate the terms of the federal and state statutes described herein.

118. An actual controversy has arisen in the wake of the data breach at issue regarding Defendant's common law and other duties to act reasonably with respect to safeguarding the payment card information belonging to Plaintiffs and the Class. Plaintiffs allege ARG's actions (and inaction) in this respect were inadequate and unreasonable and remain inadequate and unreasonable. Additionally, Plaintiffs and the Class continue to suffer injury as additional fraud and other illegal charges are being made on payment cards they issued.

119. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

(a) ARG continues to owe a legal duty to secure its customers' personal and financial information – specifically including information pertaining to credit and debit cards used by persons who made purchases at

Arby's restaurants – and to notify financial institutions of a data breach under the common law, Section 5 of the FTCA, Card Operating Regulations, PCI DSS standards, its commitments, and various state statutes;

(b) ARG continues to breach this legal duty by failing to employ reasonable measures to secure payment card information; and

(c) ARG's ongoing breach of its legal duty continues to injure Plaintiffs by subjecting them to an unreasonable risk of harm.

120. The Court should also issue corresponding injunctive relief requiring ARG to employ adequate security protocols to protect payment card information.

121. If an injunction is not issued, Plaintiffs will suffer irreparable injury and lack an adequate legal remedy in the event of another data breach of ARG's data systems. The risk of another such breach is real, immediate, and substantial. If another breach of ARG's data systems occurs, Plaintiffs will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring lawsuits to rectify the same conduct. Simply put, monetary damages, while warranted to compensate Plaintiffs for out of pocket damages that are legally quantifiable and provable, do not cover the full extent of injuries suffered by Plaintiffs, which include monetary damages that are difficult to quantify, and reputational damage.

122. The hardship to Plaintiffs and the Class if an injunction does not issue exceeds the hardship to ARG if an injunction is issued. Among other things, if ARG suffers another data breach, Plaintiffs and the members of the Class will likely incur millions of dollars in damage. On the other hand, the cost to ARG of complying with an injunction by employing reasonable data security measures is relatively minimal and ARG has a pre-existing legal obligation to employ such measures.

123. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach, thus eliminating the injuries that would result to Plaintiff, the Class, and the millions of consumers whose confidential information would be compromised.

PRAYER FOR RELIEF

124. Wherefore, Plaintiff, on behalf of itself and on behalf of the other members of the Class, requests that this Court award relief against ARG as follows:

a. Entry of an order certifying the class and designating Plaintiffs as the Class Representative and its counsel as Class Counsel;

b. An award to Plaintiffs and the proposed Class members of compensatory damages with pre-judgment and post-judgment interest;

c. Entry of a declaratory judgment in favor of Plaintiffs and the Class as described above;

d. Issuance of the injunctive relief requested above;

e. An award of attorneys' fees and costs pursuant to O.C.G.A. § 13-6-11, or as otherwise authorized by law; and

f. Such other and further relief as the Court may deem necessary or appropriate.

JURY TRIAL DEMANDED

125. Plaintiffs hereby demand a jury trial for all of the claims so triable.

Respectfully submitted this 19th day of May, 2017.

/s/ Brian C. Gudmundson
Brian C. Gudmundson
Charles S. Zimmerman
Michael J. Laird
ZIMMERMAN REED LLP
1100 IDS Center, 80 South 8th Street
Minneapolis, MN 55402
Telephone: 612.341.0400
brian.gudmundson@zimmreed.com
charles.zimmerman@zimmreed.com
michael.laird@zimmreed.com

Attorneys for Plaintiff Fort McClellan Credit Union

/s/ Kenneth S. Canfield
Kenneth S. Canfield
Ga. Bar No. 107744
DOFFERMYRE SHIELDS CANFIELD & KNOWLES, LLC
1355 Peachtree St., NE, Suite 1900
Atlanta, GA 30309
Telephone: 404.881.8900
Facsimile: 404.920.3246
kcanfield@dsckd.com

Proposed Liaison Counsel for Plaintiffs

Anthony C. Lake
Ga. Bar No. 431149
GILLEN WITHERS & LAKE, LLC
3490 Piedmont Road, N.E.
One Securities Centre, Suite 1050
Atlanta, GA 30305
Telephone: 404.842.9700
Facsimile: 404.842.9750
aclake@gwllawfirm.com

Thomas A. Withers
Ga. Bar No. 772250
GILLEN WITHERS & LAKE, LLC
8 E. Liberty Street
Savannah, GA 31401
Telephone: 912.447.8400
Facsimile: 912.629-6347
twithers@gwllawfirm.com

Karen Hanson Riebel
Kate M. Baxter-Kauf
Rachel M. Bohman
LOCKRIDGE GRINDAL NAUEN P.L.L.P.
100 Washington Ave. S.
Suite 2200
Minneapolis, MN 55401
Telephone: (612) 339-6900
Facsimile: (612-339-0981)
khriebel@locklaw.com
kmbaxte-kauf@locklaw.com
rmbohman@locklaw.com

Gary F. Lynch
Jamisen Etzel
Kevin Abramowicz
CARLSON LYNCH SWEET KILPELA & CARPENTER, LLP
1133 Penn Avenue, 5th Floor
Pittsburgh, Pennsylvania 15222
Telephone: (412) 322-9243
Facsimile: (412) 231-0246
glynch@carlsonlynch.com
jetzel@carlsonlynch.com
kabramowicz@carlsonlynch.com

Attorneys for Plaintiff MidWest America Federal Credit Union

N. Kirkland Pope
Ga. Bar No. 584255
POPE McGLAMRY, P.C.
3391 Peachtree Road, NE, Suite 300
Atlanta, GA 30326
Telephone: 404.523.7706
Facsimile: 404.524.1648
kirkpope@pmkm.com

Chris T. Hellums
Jonathan S. Mann
PITTMAN DUTTON & HELLUMS, P.C.
2001 Park Place North
1100 Park Place Tower
Birmingham, AL 35203
Telephone: 205.322.8880
Facsimile: 205.328.2711
chrish@pittmandutton.com
jonm@pittmandutton.com

Attorneys for Plaintiff Northern Alabama Educators Credit Union

Charles H. Van Horn
Ga. Bar No. 724710
Malone W. Allen
Ga. Bar No. 921070
BERMAN FINK VAN HORN P.C.
3475 Piedmont Road, NE Suite 1100
Atlanta, GA 30305
Telephone: 404.261-7711
Facsimile: 404.233.1943
cvanhorn@bfvlaw.com
mallen@bfvlaw.com

Arthur M. Murray
Caroline W. Thomas
MURRAY LAW FIRM
650 Poydras Street, Suite 2150
New Orleans, LA 70130
Telephone: 504.525.8100
Facsimile: 504.584.5249
amurray@murray-lawfirm.com
cthomas@murray-lawfirm.com

Attorneys for Plaintiff Wanigas Credit Union, Gulf Coast Bank & Trust Company, and Michigan Credit Union League

Joseph P. Guglielmo
SCOTT+SCOTT, ATTORNEYS AT LAW, LLP
230 Park Avenue, 17th Floor
New York, NY 10169
Telephone: 212.223.6444
Facsimile: 212.223.6334
jguglielmo@scott-scott.com

Erin G. Comite
Stephen J. Teti
SCOTT+SCOTT, ATTORNEYS AT LAW, LLP
156 South Main St.
P.O. Box 192
Colchester, CT 06415
Telephone: 860.537.5537
Facsimile: 860.537.4432
ecomite@scott-scott.com
steti@scott-scott.com

Attorneys for Plaintiff First Choice Federal Credit Union

Karen S. Halbert
Mike L. Roberts
ROBERTS LAW FIRM, P.A.
20 Rahling Circle
PO Box 241790
Little Rock, AR 72223
Telephone: 501.821.5575
Facsimile: 501.821.4474
mikeroberts@robertslawfirm.us
karenhalbert@robertslawfirm.us

Bryan L. Bleichner
CHESTNUT CAMBRONNE
17 Washington Avenue North
Suite 300
Minneapolis, MN 55401
Telephone: 612.339.7300
Facsimile: 612.336-2940
bbleichner@chestnutcambronne.com

Attorneys for Plaintiff Alcoa Community Federal Credit Union

James J. Pizzirusso
Swathi Bojedla
HAUSFLED LLP
1700 K. Street, NW
Suite 650
Washington, DC 20006
Telephone: 202.540.7200
Facsimile: 202.540.7201
jpizzirusso@hausfeld.com
sbojedla@hausfeld.com

W. Pitts Carr
CARR & WEATHERBY, LLP
10 North Parkway Square
4200 Northside Parkway
Atlanta, GA 30327
Telephone: 404.442.9000
Facsimile: 404.442.9700
pcarr@wpcarr.com

Attorneys for Plaintiff Valley Federal Credit Union of Montana

W. Pitts Carr
Ga. Bar No. 112100
Alex D. Weatherby
Ga. Bar No. 819975
CARR & WEATHERBY, LLP
10 North Parkway Square
4200 Northside Parkway, NW
Atlanta, GA 30327
Telephone: 404.442.9000
Facsimile: 404.442.9700
pcarr@wpcarr.com
aweatherby@wpcarr.com

Jonathan L. Kudulis
KUDULIS REISINGER PRICE
17 North 20th Street, Suite 350
Birmingham, AL 35203
Telephone: 205.251.3151
Facsimile: 205.322.6444
jkudulis@trimmier.com

Attorneys for Plaintiff Fort McClellan Credit Union

CERTIFICATION

The undersigned hereby certifies, pursuant to Local Rule 7.1(D), that the foregoing document has been prepared with one the font and point selections (Times New Roman, 14 point) approved by the Court in Local Rule 5.1(C).

/s/ Brian C. Gudmundson
Charles S. Zimmerman
Brian C. Gudmundson
Michael J. Laird
ZIMMERMAN REED LLP
1100 IDS Center, 80 South 8th Street
Minneapolis, MN 55402
Telephone: 612.341.0400
charles.zimmerman@zimmreed.com
brian.gudmundson@zimmreed.com
michael.laird@zimmreed.com

CERTIFICATE OF SERVICE

I hereby certify that on May 19, 2017, I electronically filed the foregoing document by using the CM/ECF system, which will send notification of such filing to all counsel of record.

/s/ Brian C. Gudmundson
Brian C. Gudmundson